UNIT –0 3

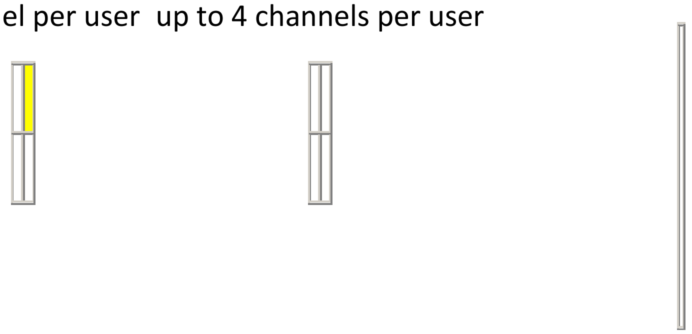
ALOHA

Unit-03/Lecture-01/ Lecture-02

Static Channel Allocation in LANs and MANs[RGPV/Jun 2010, Jun2014]

- **Frequency Division Multiplexing -** Frequency of one channel divided (usually evenly) among n users. Each user appears to have full channel of full frequency/n. Wastes bandwidth when user has nothing to send or receive, which is often the case in data communications. Other users cannot take advantage of unused bandwidth.
- **Time Division Multiplexing** - Time of one channel divided (usually evenly) among n users. Each user appears to have full channel for time/n. same problems as FDM.
- **Analysis of Static Channel Allocation -** Static allocation is intuitively a bad idea when considering that for an n divisions of a channel, any one user is limited to only 1/n channel bandwidth whether other users where accessing the channel or not. By limiting a user to only a fraction of the available channel, the delay to the user is increased over that if the entire channel were available.
  Intuitively, static allocation results in restricting one user to one channel even when other channels are available. Consider the following two diagrams, each with one user wanting to transmit 400 bits over a 1 bit per second channel. The left diagram would have a delay 4 times greater than the diagram on the right, delaying 400 seconds using 1 channel versus 100 second delay using the 4 channels.

Static Allocation 1 channel per user	Dynamic Allocation up to 4 channels per user	One user with entire channel



Generally we want delay to be small. More formally the mean time delay for one channel, T is:

C = Channel capacity bps (constant). Larger capacity reduces T.
l = input rate, frames/sec. Smaller input rate reduces T.
m = average bits per frame. Larger frames reduces T.
T = 1/ (mC-l) mean time delay

For each of n sub channels, the mean delay time using FDM (T_{FDM}) is:

C/n = Channel capacity bps (constant)
l/n = input rate, frames/sec.
m = average bits per frame

$$T_{FDM} = 1/ (m(C/n)-(l/n)) = n/(mC-l) = nT$$

Generally, dividing a channel statically into n channels increases the average delay by a factor of n agreeing with the intuitive result from the diagrams.

Dynamic Channel Allocation in LANs and MANs - Obviously static allocation of a multi-access channel is not generally desirable when overall channel usage is low. Note that channel use is bursty with long periods of inactivity punctuated by short bursts of activity.

Dynamic Channel Allocation Assumptions

- **Station model -** n independent stations each generating frames for transmission. One frame is generated and successfully transmitted at a time.
- **Single channel -** A single channel is shared with other stations.
- **Collision -** Overlapping transmissions destroy the frames, can be detected, and require retransmission. Collisions are the only errors.
- **Time**
  - **Continuous time -** No master clock dividing time, transmissions can begin at any time.
  - **Slotted time -** Master clock, time is divided into discrete intervals (slots), transmissions can only begin at the start of a slot. Slots may contain 0 frames (idle), 1 (a successful transmission), or 2 (a collision).
- **Carrier**
  - **Carrier sense -** Stations can detect whether the channel is in use prior to transmitting. If in use waits for channel to become available.
  - **No carrier sense -** Stations cannot detect whether the channel is in use prior to transmitting. Transmits and later determines whether successful.

ALOHA [RGPV/ Dec 2009,Jun 2010, Dec 2010,Dec 2013,Jun 2014]

ALOHA, the earliest random access method was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. The idea is that each station sends a frame whenever it has a frame to send.

However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure shows an example of frame collisions in pure ALOHA.

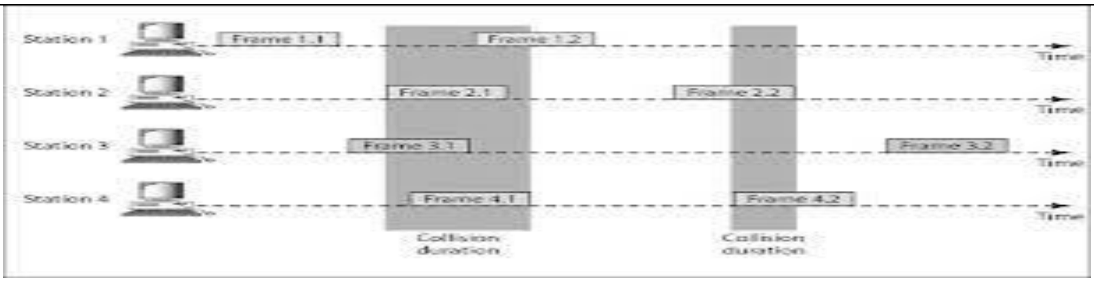


FIGURE 3.1: PURE ALOHA

There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.

It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver.

When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time TB.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later.

The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Tp)' The back-off time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. One common formula is the **binary exponential back-off.** In this method, for each retransmission, a multiplier in the range 0 to 2K - 1 is randomly chosen and multiplied by Tp (maximum propagation time) or Tfr (the average time required to send out a frame) to find TB' Note that in this procedure, the range of the random numbers increases after each collision. The value of Kmax is usually chosen as 15.

Vulnerable time Let us find the length of time, the **vulnerable time,** in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking Tfr S to send. Figure 12.5 shows the vulnerable time for station A.

Vulnerable time = 2 X Tfr

Station A sends a frame at time t. Now imagine station B has already sent a frame between t - Tfr and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame. On the other hand, suppose that station C sends a frame between t and t

+ Tfr . Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

We see that the vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

Pure ALOHA vulnerable time = 2 x Tfr

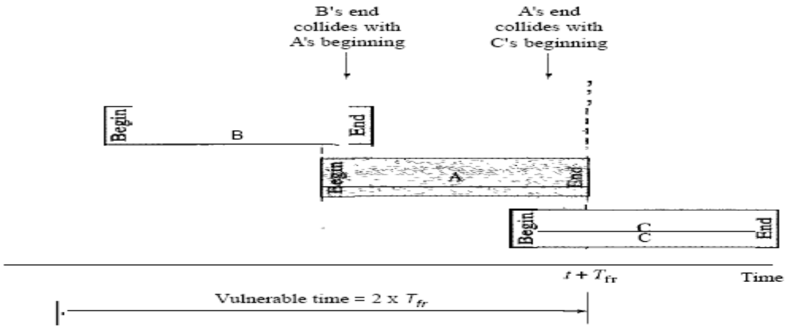

B's end collides with A's beginning
A's end collides with C's beginning
Begin
B
End
Begin
A
End
Begin
C
End
$t + T_{fr}$
Time
Vulnerable time = 2 x T_{fr}

FIGURE 3.2: VULNERABLE TIME PURE ALOHA

Throughput Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average number of successful transmissions for pure ALOHA is S = G x e-2G.
he maximum throughput Smax is 0.184, for G = 1.
In other words, if one-half a frame is generated during one 2 frame transmission time (in other words, one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully. This is an expected result because the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.
The throughput for pure ALOHA is S =G x e-2G.
The maximum throughput Smax =0.184 when G = (1/2).

Slotted ALOHA
Pure ALOHA has a vulnerable time of 2 x Tfr . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot. Figure shows an example of frame collisions in slotted ALOHA.

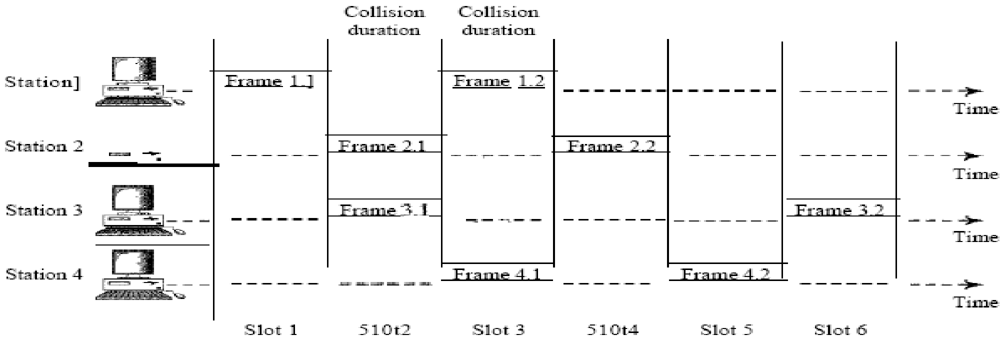


FIGURE 3.3: SLOTTED ALOHA

Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to Tfr.
It shows that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

Slotted ALOHA vulnerable time = Tfr
Throughput It can be proved that the average number of successful transmissions for slotted ALOHA is S = G x e-G. The maximum throughput Smax is 0.368, when G = 1.
In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.
The throughput for slotted ALOHA is S =: G x e-G.
The maximum throughput Smax == 0.368 when G=1.
Vulnerable time for slotted ALOHA protocol= Tfr

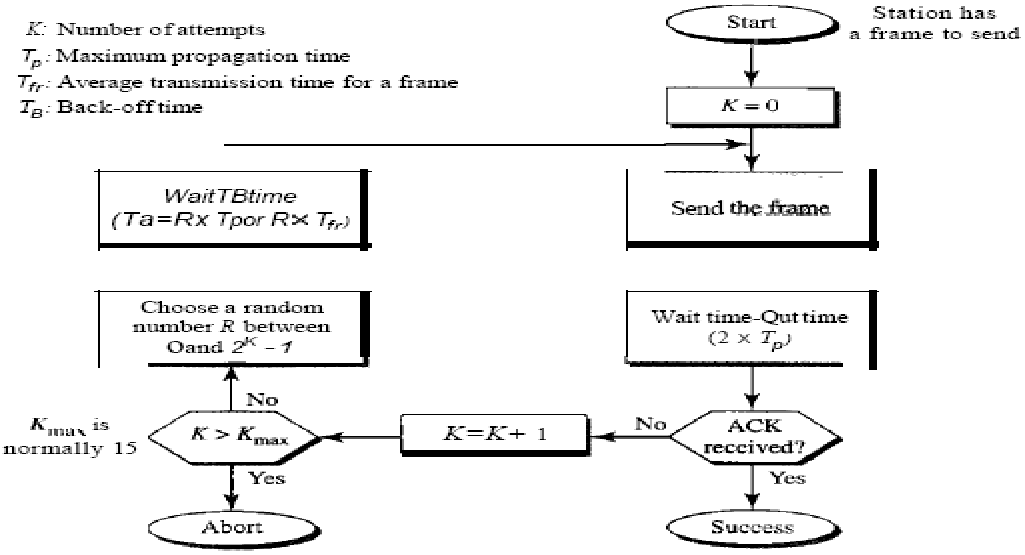

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Start
Station has a frame to send
K = 0
WaitTBtime (Ta=Rx Tpor R× T_{fr})
Send the frame
Choose a random number R between Oand $2^K - 1$
Wait time-Qut time ($2 \times T_p$)
No
K_{max} is normally 15
$K > K_{max}$
K=K+ 1
No
ACK received?
Yes
Yes
Abort
Success

FIGURE 3.4: ALOHA FLOW DIAGRAM

Comparison between pure and slotted aloha

ALOHA is a medium access protocol that was originally designed for ground based radio broadcasting however it is applicable to any system in which uncoordinated users are competing for the use of a shared channel. Pure ALOHA and slotted ALOHA are the two versions of ALOHA.

Pure ALOHA uses a very simple idea that is to let users transmit whenever they have data to send. Pure ALOHA is featured with the feedback property that enables it to listen to the channel and finds out whether the frame was destroyed. Feedback is immediate in LANs but there is a delay of 270 msec in the satellite transmission. It requires acknowledgment if listening to the channel is not possible due to some reason. It can provide a channel utilization of 18 percent that is not appealing but it gives the advantage of transmitting any time.

Slotted ALOHA divides time into discrete intervals and each interval corresponds to a frame of data. It requires users to agree on slot boundaries. It does not allow a system to transmit any time. Instead the system has to wait for the beginning if the next slot.

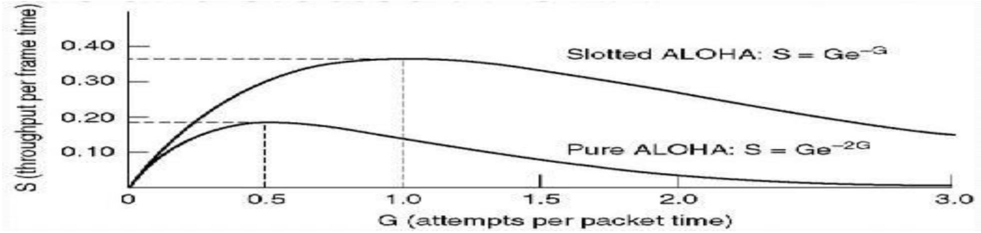


FIGURE 3.5: THROUGHPUT ALOHA

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is static & dynamic allocation?	Jun 2010	7
Q.2	Write short note on ALOHA?	Dec 2003 June2005	7
Q.3	Derive an expression to prove that throughput of Slotted Aloha is approximately twice than that of Pure Aloha?	JUN 2004 Dec 2006	7

		Jun 2009 Dec 2010 Jun 2011	
Q.4	Derive a relationship between offered traffic and throughput in Slotted Aloha.	Jun 2006	7
Q.5	A pure aloha network transmits 200 bits frames on a shared channel of 200 kbps. What is the throughput if the system produces 1000 frames/second?	Dec 2013	7
Q.6	Define the throughput of pure aloha? A pure aloha network transmits 200 bit frames on a shared channel of 200kbps. What is the throughput if the system(all station together) produces- (i) 1000 frames per second (ii) 500 frames per second (iii) 250 frames per second	Jun 2013	7
Q.7	Name different types of static and dynamic channel allocation policies of MAC sublayer. Compare static and dynamic channel allocation strategies under the heading of advantaged and disadvantages.	Jun 2014	7
Q.8	Explain giving neat sketches pure and slotted ALOHA?	Jun 2014	7

Unit-03/Lecture-03

CSMA

Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle **"sense before transmit"** or **"listen before talk."**

CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason is, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).
The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station

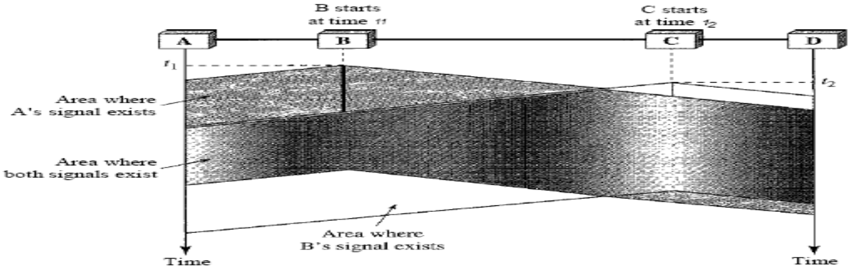


FIGURE 3.6: CSMA

Vulnerable Time

The vulnerable time for CSMA is the propagation time Tp . This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

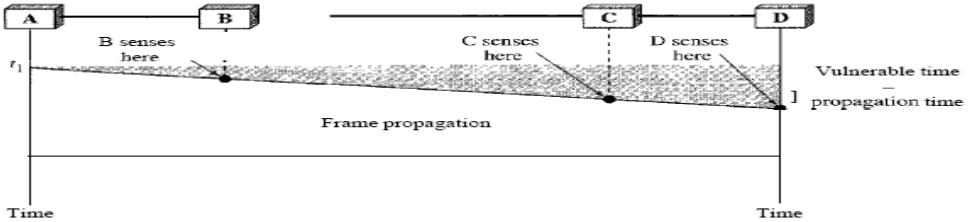


FIGURE 3.7: VULNERABLE TIME CSMA

Persistent Method

- **1-Persistent** 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

- **Nonpersistent** In the nonpersistent method**,** a station that has a frame to send senses the line. If the line is idle, it sends immediately.

- **P-Persistent The p-persistent method** is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:
  1. With probability p, the station sends its frame.
  2. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
     a. If the line is idle, it goes to step 1.
     b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

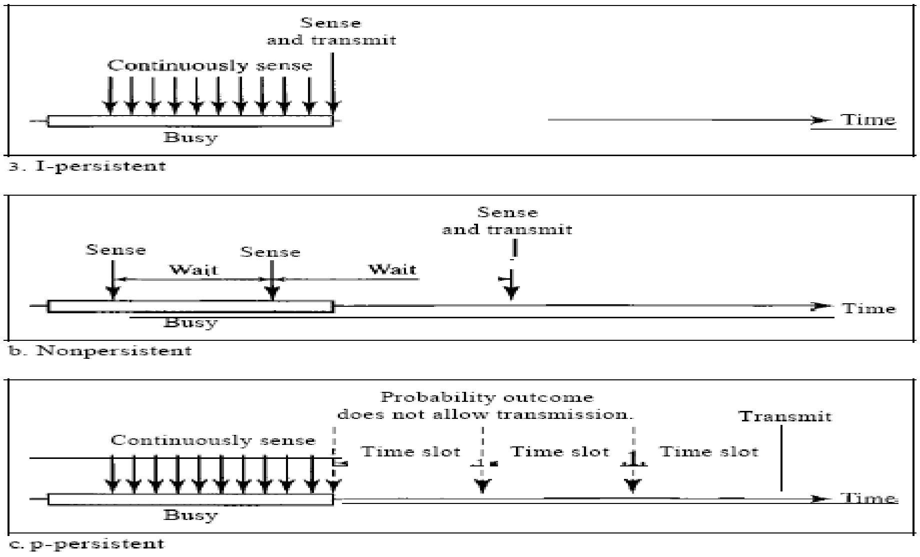


FIGURE 3.8: PERSISTENT METHOD CSMA

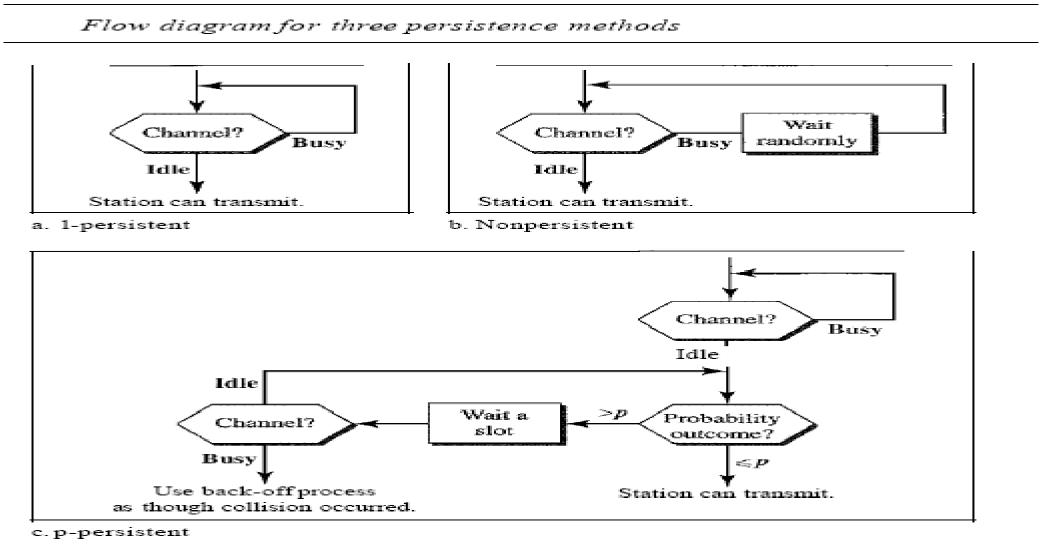


FIGURE 3.9: PERSISTENT METHOD FLOE DIAGRAM

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the following CSMA protocol- (i)1 persistent (ii) p-persistent (iii) non-persistent	Dec.2003 Dec 2006 Dec 2011	7
Q.2	In p-persistent CSMA the value of p is wrongly estimated. How will it affected the network performance?	June.2013	7
Q.3	Explain CSMA protocols & give their best channel utilization.	Dec.2011	7

Unit-03/Lecture-05

CSMA / CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

Collisions are avoided through the use of CSMA/CA's three strategies:

- The Interframe Space(IFS)
- The Contention Window
- Acknowledgments

Interframe Space (IFS)

First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.

The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time (described next). The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned shorter IFS has a higher priority.

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

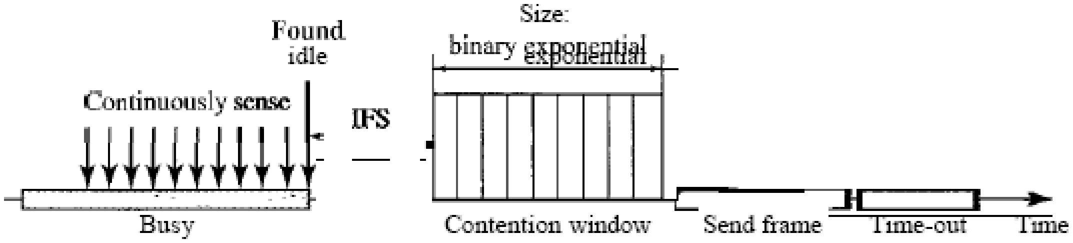


FIGURE 3.12: CSMA/CA

Contention Window

The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time. In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Procedure

The channel needs to be sensed before and after the IFS. The channel also needs to be sensed during the contention time. For each time slot of the contention window, the channel is sensed. If it is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.

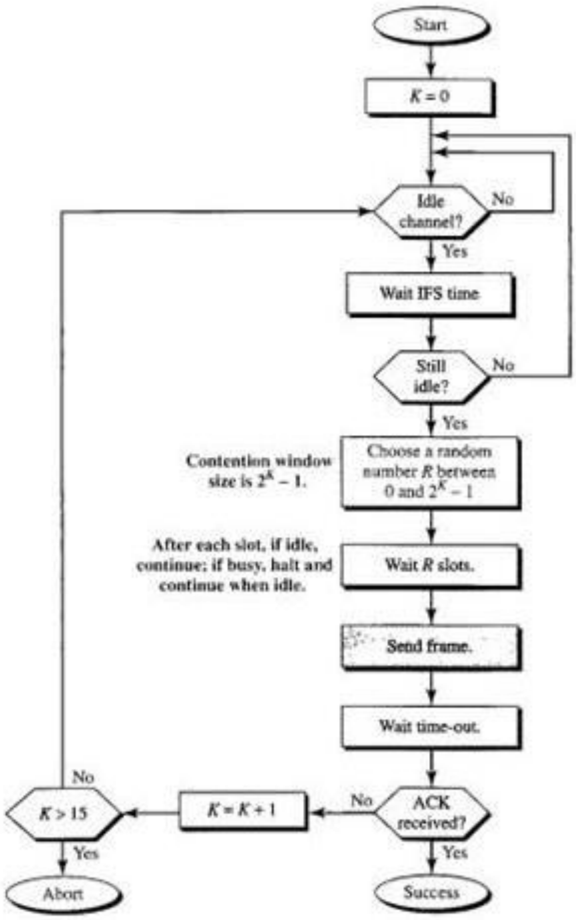

Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is 2^K – 1.
Choose a random number R between 0 and 2^K – 1
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
No
K > 15
K = K + 1
No
ACK received?
Yes
Yes
Abort
Success

FIGURE 3.13: CSMA/CA FLOW DIAGRAM

UNIT 03/LECTURE 06

IEEE 802.4 TOKEN BUS

Token bus network[RGPV/ Dec 2009, Dec 2012]

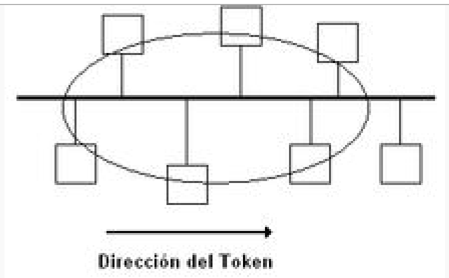


FIGURE 3.14: TOKEN PASSING IN A TOKEN BUS NETWORK

Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable. A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbor in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

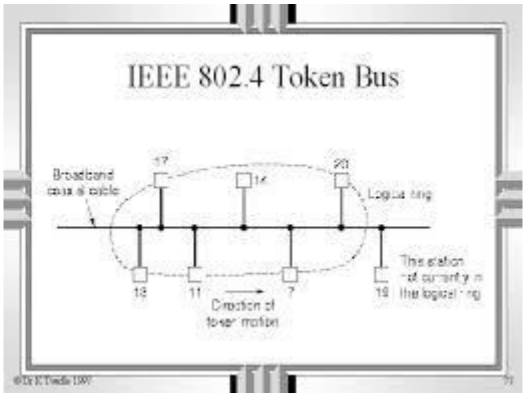


FIGURE 3.15: TOKEN BUS

Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. This is an application of the concepts used in token ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring.

Due to difficulties handling device failures and adding new stations to a network, token bus gained a reputation for being unreliable and difficult to upgrade.

Advantages and disadvantages of 802.4

Advantages

- Uses cable TV cables and parts readily and cheaply available.
- Deterministic and able to prioritize traffic.
- Short minimum frames.

- Excellent performance under conditions of high load.
- Broadband can support multiple channels (for example, video and voice)

Disadvantages

- Complex protocol and engineering of equipment.
- Expensive; requires modems and repeaters.
- Since node must wait for token to come around before transmitting, messages are delayed waiting for token even when network is idle.

Frame format

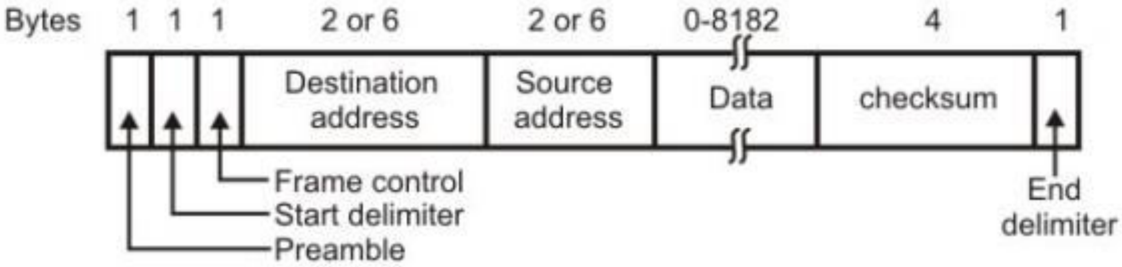


FIGURE 3.16: TOKEN BUS FRAME FORMAT

- Preamble – clock synchronization
  - Starting and ending delimiter
  - frame boundaries
    - analog encoding symbols (other than 0 or 1)
    - does not occur in analog data
  - no need of length field
  - Frame Control
    - Successors,
    - predecessors
    - Entry of new station
    - Claim token
      - Token lost, station with token dead
    - Protocols to handle all issues
    - Useful for real time traffic

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	What is 802.4? How token is passed in the ring? Give advantages and disadvantages of 802.4.	Dec 2009	7
Q.2	Write short notes on IEEE 802.4	Dec 2012	7

UNIT 03/LECTURE 07

IEEE 802.5 TOKEN RING

Star-wired ring topology

The star-wired ring topology is a circular connection of workstations. The star-wired ring is essentially a marriage of the earlier ring topology to the star-wired topology. Since star-wired ring topologies support baseband signals, the star-wired ring is capable of supporting only one channel of information. This channel of information flows in one direction around the ring, moving from workstation to workstation. Since the star-wired ring is a closed loop of wire, it is important for some device to remove a circling piece of data from the ring; otherwise, the piece of data will keep circling. The device that removes the data is the workstation that originally transmitted the data.

Although the logical organization of the workstations in a star-wired ring topology is circular, the physical organization of a star-wired ring is not circular. Physically, a star-wired ring looks much like a star-wired bus design, with all its workstations connected to a central device. This central device is not a hub but a multistation access unit. A Multistation Access Unit (MAU) accepts data from a workstation and transmits this data to the next workstation downstream in the ring.

An MAU is quite a bit different from a hub in that it does not send a copy of the incoming data immediately out to every connection. If a workstation is not connected to a particular port on the MAU, that port simply closes itself so that a continuous ring is maintained. Thus, a ring topology based on MAUs is commonly referred to as a star-wired ring topology. As with hubs in the star-wired bus design, it is possible to interconnect multiple MAUs to extend the size of a star-wired ring local area network. As the data passes around the ring in the first MAU, it encounters the connector to the second MAU. The signal then passes over the cable to the second MAU and begins its journey around the ring in the second MAU. When all workstations have been accessed on the second MAU, the signal passes again over the cable and returns to the first MAU.

The star-wired ring topology has many of the same advantages as the star-wired bus topology. The star-wired ring topology is based on twisted pair wiring, and because it makes installing new workstations easy, it is easy to maintain. Some of the disadvantages of star-wired rings include slower transmission speeds, higher costs, and more complex software. Because of these disadvantages, and the fact that star-wired buses have pretty much taken over the local area network market, the star-wired ring is close to extinction.

Token Ring

The token ring local area network uses the star-wired ring topology for the hardware and a round robin protocol for the software. It operates on the principle that to transmit data onto the ring, your workstation must be currently in possession of software token. There is typically only one token in the entire network, so only one workstation may transmit at a time. When a workstation has completed its transmission, it passes the token on to the downstream neighboring workstation. Only the workstation holding the token can transmit, so there is no need for any workstation to listen for a collision while transmitting, because collisions cannot occur.

As has been mentioned, collisions are one of the main problems of CSMA/CD. As the number of concurrent users rises, the number of collisions rises. As the collisions rise, more workstations are forced to retransmit their messages, and overall throughput declines. Since the token ring does not experience any collisions, overall throughput remains high even under heavy loads. This ability of token ring to give every workstation a turn is attractive and is valuable for applications that require uniform response times. Since the order of transmission by each workstation is known, the wait time to transmit can be determined (as opposed to being unpredictable); thus, token ring is a deterministic protocol.

Let's take a quick look at how the token ring protocol works. Consider, in which Station A has just released the token. Since Station B is the next downstream neighbor from Station A, and Station B has data to transmit on the ring, Station B seizes the token. After seizing the token, Station B transmits its data, which is destined for Station M. As Station M copies in the data frame, the data continues around the ring until it returns to Station B, which removes the data from the ring. After Station B has removed its data from the ring, it passes the token to Station C.

Frame format

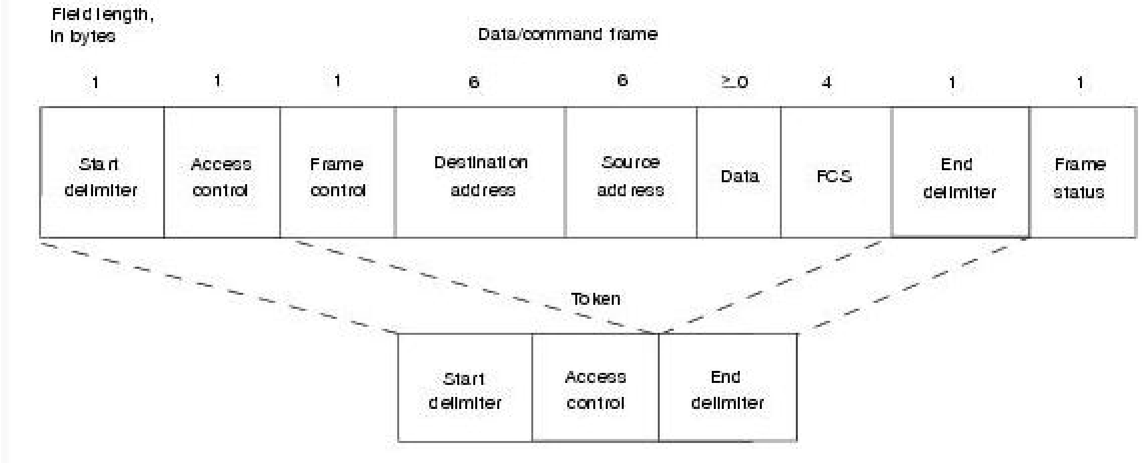


FIGURE 3.17: TOKEN RING FRAME FORMAT

Token Frame Fields

The three token frame fields are summarized in the descriptions that follow:

- **Start delimiter** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **End delimiter** - Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described in the following summaries:

- **Start delimiter** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **Frame-control bytes** Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data** Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS)** is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter** Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame Status** is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Advantages and disadvantages of 802.5

A major disadvantage of the token ring access protocol is the complexity of the software needed to maintain the token. This software has to address important questions such as:

- What happens if the token disappears? (A workstation does not forward it)
- If the token disappears, who generates a new token?
- Is it possible for two stations to generate a token, thus resulting in two tokens on the ring?

Although token ring has the definite advantage of being a deterministic protocol and performing quite well under heavy loads, it has had a difficult time competing with CSMA/CD networks. An overwhelming majority of local area networks use CSMA/CD as the medium access control protocol of choice. Some reasons that CSMA/CD is more popular than token ring are:

- CSMA/CD was the first local area network medium access control method, and thus got a good jump on installations and support.
- Token ring local area networks have almost always lagged behind CSMA/CD networks with regard to transmission speed. When CSMA/CD first became popular, the typical transmission speed

was 10 Mbps. Token ring, when it first appeared, had a transmission speed of only 4 Mbps. For a while, token ring jumped ahead with a 16-Mbps version, but CSMA/CD caught up with a 100-Mbps version, and then a 1000-Mbps version. Token ring finally announced a 100-Mbps version, but this was too late to save the protocol in the marketplace. Many people feel it will just be a matter of time before token ring fades into the history books.

- CSMA/CD is less expensive to implement, due in part to its widespread marketing and acceptance. CSMA/CD is a simpler protocol.

Comparison of IEEE 802.3, IEEE 802.4 and IEEE 802.5 Standards

Sr.No	**Parameter of comparison**	**802.3 Ethernet**	**802 4Token Bus**	**802.5Token Ring**
1	Physical topology	Linear	Linear	Ring
2	Logical topology	None	Ring	Ring
3	Contention	Random chance	By token	By token
4	Adding stations	A new station can be added almost anywhere on the cable at any time.	Distributed algorithms are needed to add new stations.	Must be added between two specified stations.
5	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce the effective data to nearly 0.	Stations must wait for the token even if no other station is transmitting. Under heavy load, token passing provides fair access to all stations.	Stations must wait for the token even if no other station is transmitting. Under heavy loads, token passing provides fair access to all stations.
6	Maximum delay before transmitting	None	Bounded, depending on distance spanned and number of stations.	Bounded, depending on distance spanned and number of stations. However, if priorities are used, a low priority station may have no maximum delay.
7	Maintenance	No central maintenance	Distributed algorithm provide maintenance	A designated monitor station performs

				maintenance.
8	Cable used	Twisted pair, co-axial fiber optic	co axial	Twisted pair and fiber optic.
9	Cable length	50 to 2000 m	200 to 500 m	50 to 2000 m
10	Frame	l0Mbps to 100 Mbps	10Mbps	4 to l00Mbps
11	structure	1500 bytes	8191 bytes	5000 bytes

NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain the working of IEEE 802.5 with the help of neat diagram. Give two reasons why not to choose token ring.	Dec 2010	7
Q.2	Discuss the compare IEEE 802.3, IEEE 802.4 and IEEE 802.5 Standards	Jun 2004	7

UNIT 03/LECTURE 08

FDDI

Fiber Distributed Data Interface (FDDI)[RGPV/Dec 2009, Jun 2011, Dec 2011, Dec 2012, Jun 2013]
Fiber distributed data interface (FDDI) is a local area network protocol standardized by ANSI and the ITU- T (ITU- T X.3). It supports data rates of 100 Mbps and provides a high-speed alternative to Ethernet and Token Ring. When FDDI was designed, speeds of 100 Mbps required fiber-optic cable. Today, however, comparable speeds are available using copper cable. The copper version of FDDI is known as CDDI.

Access Method: Token Passing

In FDDI, access is limited by time. A station may send as many frames as it can within its allotted access period, with the proviso that real-time data be sent first.

To implement this access mechanism, FDDI differentiates between two types of data frames: synchronous and asynchronous. Synchronous here refers to information that is real-time, while asynchronous refers to information that is not. These frames are usually called S-frames and A-frames.

Each station that captures the token is required to send S-frames first. In fact, it must send its S-frames whether or not it's time allotment has run out. Any remaining time may then be used to send A-frames. To understand how this mechanism ensures fair and timely link access, it is necessary to understand the FDDI time registers and timers.

Time Registers

FDDI defines three time registers to control circulation of the token and distribute link access opportunities among the nodes equitably. Values are set when the ring is initialized and do not vary in the course of operation. The registers are called synchronous allocation (SA), target token rotation time (TTRT), and absolute maximum time (AMT).

- **Synchronous Allocation (SA)** The SA register indicates the length of time allowed each station for sending synchronous data. This value is different for each station and is negotiated during initialization of the ring.

- **Target Token Rotation Time (TTRT)** The TTRT register indicates the **average time required** for a token to circulate around the ring exactly once (the **elapsed time between a token's arrival at a given station and its next arrival at the same station**). Because it is an **average**, the actual time of any rotation may be greater or less than this value.

- **Absolute Maximum Time (AMT)** The AMT register holds a value equal to twice the TTRT. A token may not take longer than this time to make one rotation of the ring. If it does, some station or stations are monopolizing the network and the ring must be reinitialized.

Timers

Each station contains a set of timers that enable it to compare actual timings with the values contained in the registers. Timers can be set and" reset, and the_ values decremented or incremented at a rate set by the system clock. The two timers used by FDDI are called the token rotation timer (TRT) and token holding timer (THT).

- **Token Rotation Timer (TRT)** The TRT runs continuously and measures the **actual time** taken by the token to complete a cycle. In our implementation, we use an incrementing TRT for simplicity, although some implementations may use a decrementing timer.

- **Token Holding Timer (THT)** The THT begins running as soon as the token is received. Its function is to show how much time remains for sending asynchronous frames once the synchronous frames have been sent. In our implementation, we use a decrementing THT for simplicity, although some implementations may use an incrementing one. In addition, we allow the value of THT to become negative (to make the concept easier to understand) although a real timer may stay at zero.

Station Procedure

When a token arrives, each station follows this procedure:
1. THT is set to the difference between TTRT and TRT (THT = TIRT - TRT).
2. TRT is reset to zero (TRT = 0).
3. The station sends its synchronous data.
4. The station sends asynchronous data till the value of THT is positive.

Addressing

FDDI uses a six-byte address, which is imprinted on the NIC card similar to Ethernet addresses.

Electrical Specification

Signaling (Physical Layer)

FDDI uses a special encoding mechanism called four bits/five bits (4B/5B). In this system, each four-bit segment of data is replaced by a five-bit code before being encoded in NRZ-I. The NRZ-I used here inverts on the 1.

Encoding

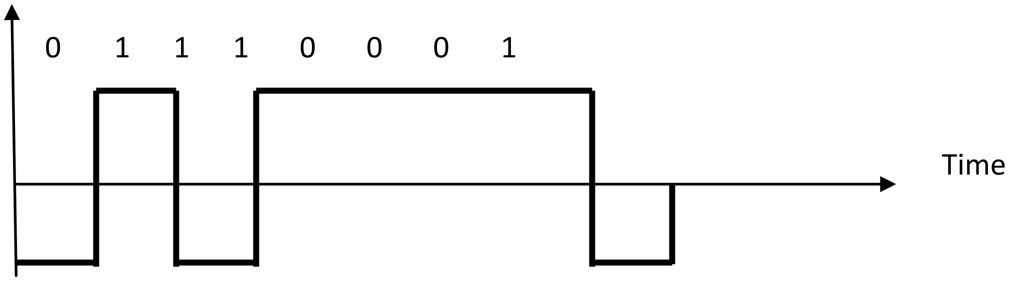


FIGURE 3.18: FDDI

The reason for this extra encoding step is that, although NRZ-I provides adequate synchronization under average circumstances, sender and receiver may go out of synchronization anytime the data includes a long sequence of 0s. 4B/5B encoding transforms each four-bit data segment into a five bit unit that contains no more than two consecutive 0s. Each of the 16 possible four-bit patterns is assigned a five-bit pattern to represent it. These five-bit patterns have been carefully selected so that even sequential data units cannot result in sequences of more than three 0s (none of the five-bit patterns start with more than one 0 or end with more than two 0s);

Data Rate
FDDI supports data rates up to 100 Mbps.

Frame Format

The FDDI standard divides transmission functions into four protocols: physical medium dependent (PMD), physical (PHY), media access control (MAC), and logical link control (LLC). These protocols correspond to the physical and data link layers of the OSI model. In addition, the standard specifies a fifth protocol (used for station management).

FDDI Layers

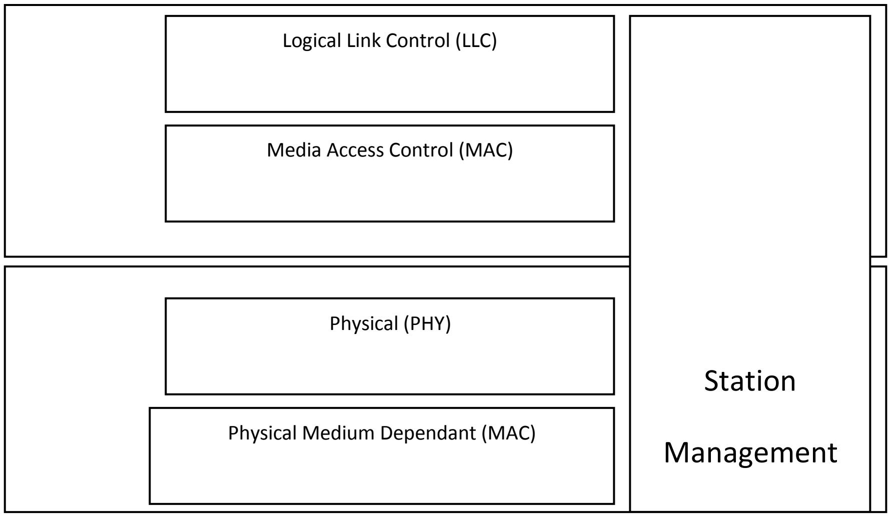

Logical Link Control (LLC)
Media Access Control (MAC)
Physical (PHY)
Physical Medium Dependant (MAC)
Station
Management

FIGURE 3.19: FDDI LAYER

Logical Link Control
The LLC layer is similar to that defined in the IEEE 802.2 protocols.

Media Access Control
The FDDI MAC layer is almost identical to that defined for Token Ring. However. although the functions are similar, the FDDI MAC frame itself is different enough to warrant an independent discussion of each field

Each frame is preceded by 16 idle symbols (1111), for a total of 64 bits to initialize clock synchronization with the receiver.

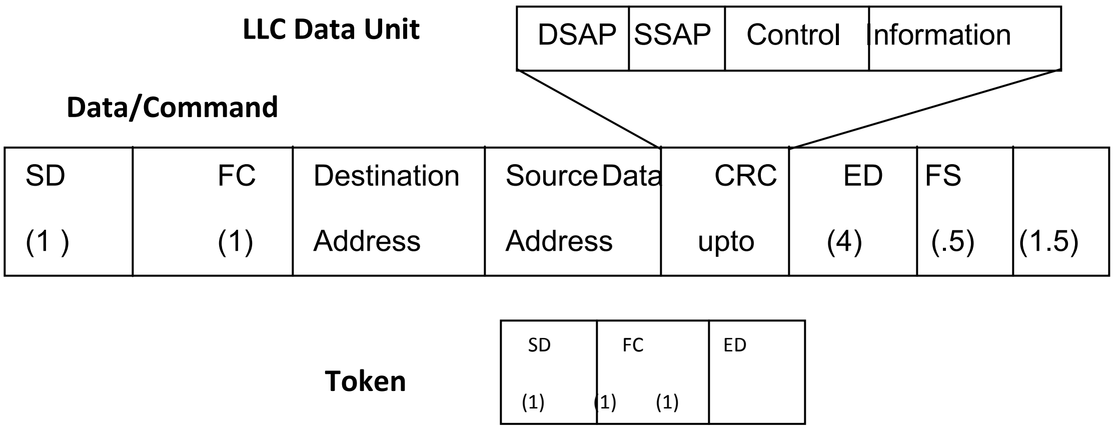


FIGURE 3.20: FDDI MAC LAYER

SD : Start Delimiter (flag)
FC : Frame Control (frame type)
ED : End Delimiter (flag)
CRC : Cyclic Redundancy Check
FS : Frame status

Frame Fields There are eight fields in the FDDI frame:

- **Start delimiter (SD)** The first byte of the field is the frame's starting flag. As in **Token Ring**, these bits are replaced in the physical layer by the control codes (violations) J and K (the five-bit sequences used to represent J and K are shown in Table 4B/5B Control Symbols.
- **Frame control (FC)** The second byte of the frame identifies the frame type.
- **Addresses** The next two fields are the destination and source addresses. Each address consists of two to six bytes.
- **Data** Each data frame can carry up to 4500 bytes of data.
- **CRC** FDDI uses the standard IEEE four-byte cyclic redundancy check.
- **End delimiter (ED)** This field consists of half a byte in the data frame or a full byte in the token frame. It is changed in the physical layer with one violation symbol in the data/command frame or two T symbols in the token frame. (Refer 4B/5B Control Symbols)
- **Frame status (FS)** The FDDI FS field is similar to that of Token Ring. It is included only in the data/command frame and consists of 1.5 bytes.

Implementation: Physical Medium Dependent (PMD) Layer

The physical medium dependent (PMD) layer defines the required connections and electronic components. Specifications for this layer depend on whether the transmission medium used is fiber-optic or copper cable.

Dual Ring

FDDI is implemented as a dual ring. In most cases, data transmission is confined to the primary ring. The secondary ring is provided in case the primary fails.

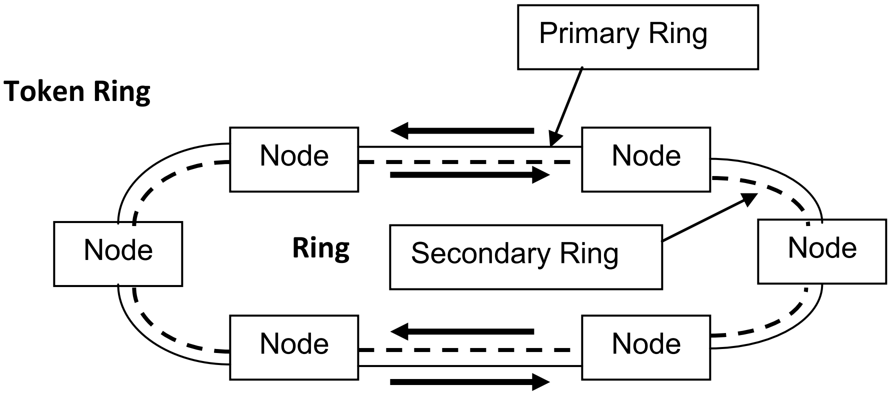


FIGURE 3.21: FDDI DUAL RING

The secondary ring makes FDDI self-healing. Whenever a problem occurs on tile primary ring, the secondary can be activated to complete data circuits and maintain service.

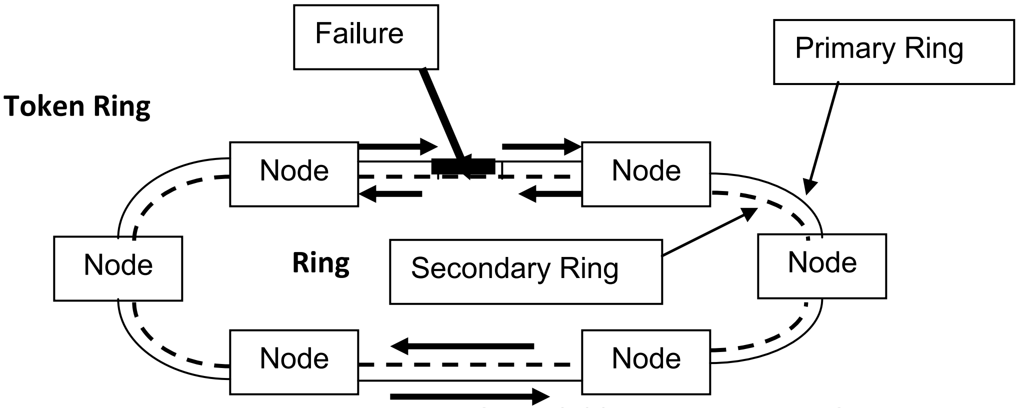


FIGURE 3.22: FDDI DUAL RING FAILURE

Nodes connect to one or both rings using a **media interface connector** (MIC) that can be either male or female depending on the requirements of the station.

Advantage and disadvantage of FDDI

Advantages:

- FDDI supports real-time allocation of network bandwidth.
- This allows you to use a wide array of different types of traffic.
- FDDI has a dual ring that is fault-tolerant. The benefit here is that if a station on the ring fails or if the cable becomes damaged, the dual ring is automaticaly doubled back onto itself into a single ring.
- The FDDI compensates for wiring failures. The stations wrap within themselves when the wiring fails.
- Optical bypass switches are used that can help prevent ring segmentation. The faild stations are eliminated from the ring.

Disadvantages:

- There's a potential for multiple ring failures.
- As the network grows, this possibility grows larger and larger.
- The use of fiber optic cables is expensive.
- This has kept many companies from deploying FDDI in a widespread manner. Instead, they have been using copper wire and the similar method of CDDI.

COMPARISON

Ethernet is good for low-level loads but collapses as the load increases due to collisions and retransmissions. Token Ring and fool perform equally well at low- and high-level loads.

Network	**Access Method**	**Signaling**	**Data** **Rate**	**Error** **Control**
Ethernet	CSMA/CD	Manchester	1,10 Mbps	No
Fast Ethernet	CSMA/CD	Several	100 Mbps	No
Gigabit Ethernet	CSMA/CD	Several	1 Gbps	No
Token Ring	Token passing	Differential Manchester	4, 16 Mbps	Yes
FDDI	Token passing	4B/5B, NRZ-I	100 Mbps	Yes

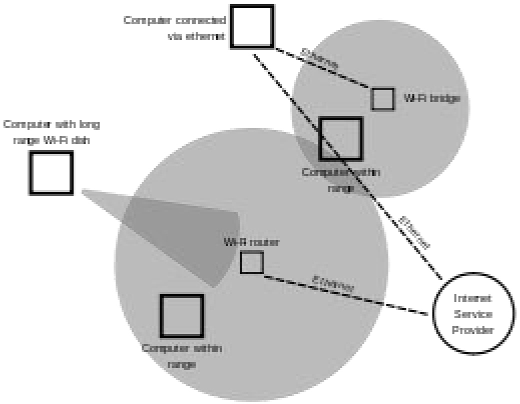
S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Write short notes on FDDI protocol.	Jun 2011 Dec 2012	7
Q.2	Compare the capacity allocation schemes for IEEE 802.5 token ring and FDDI. What are the relative pros & cons?	Dec 2011	7
Q.3	Explain FDDI network. What is the protocol used to MAC layer of FDDI LANS?	Dec 2009	7
Q.4	Explain the concept of FDDI wireless LAN in communication.	Jun 2013	7

UNIT 03/ LECTURE- 09/ LECTURE- 10

WIRELESS LAN

Wireless LAN[RGPV/ Jun 2010, Jun 2011, Dec 2012, Dec 2013, Jun 2014]

A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.


Computer connected via ethernet
Ethernet
Wi-Fi bridge
Computer with long range Wi-Fi dish
Computer within range
Ethernet
Wi-Fi router
Ethernet
Internet Service Provider
Computer within range

Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free.

Stations

All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface controllers(WNICs). Wireless stations fall into one of two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops,personal digital assistants, IP phones and other smartphones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

Extended service set

An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: ad hoc mode and infrastructure mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms:Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

Wireless distribution system

A Wireless Distribution System enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. WDS also requires that every base station be configured to forward to others in the system as mentioned above.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is halved for all clients connected wirelessly.

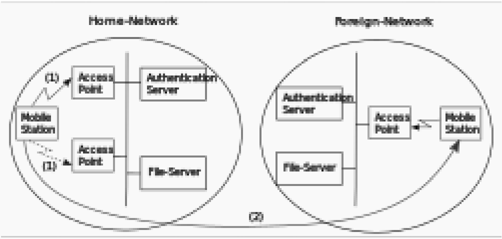
When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

Roaming

Roaming among Wireless Local Area Networks

There are two definitions for wireless LAN roaming:

- Internal Roaming (1): The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak. An authentication server (RADIUS) performs the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data among the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based on proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. External Roaming (2): The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.



Applications

Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains. Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid.

Comparison of wired and wireless LAN

Wired Network

- Wired networking requires cables to be connected to each and every computer in the network
- Cost of a Wired network is less as compared to wireless network as Ethernet ,cables, switches are not expensive
- Wired LAN offers better performance as compared to wireless networks. Wired network can offer 100Mpbs bandwidth using Fast Ethernet technology.
- Ethernet cables, Switches are used in wired network are reliable.
- Security considerations for a wired network connected to the internet are firewalls. Firewall software can be installed on each computer.

Wireless Network

- Wireless network can be configured in two ways. I.e. Adhoc or infrastructure mode. Wireless devices require WLAN cards and access points for communication.

- Wireless networks require equipments like Wireless Adapters and access points which quite expensive.

- Cost of wireless networks is high as compared to wired networks.
  Maximum bandwidth provided by wireless network is about 11Mpbs.

- The reliability of wireless network is less as compared to wired network.

- WLANS use wired equivalent privacy (WEP) encryption to protect the data. This makes wireless networks as secure as wired networks.

- Laptops and other computing devices can be moved around freely within the wireless network because mobility of wireless network is better as compared to wired networks.

WLAN vs. LAN

LAN stands for Local Area Network, which is a collection of computers and other network devices in a certain location that are connected together by switches and/or routers that facilitate the communication of the network elements. Each computer or network element is connected to the switches/routers via a UTP cable. The added letter in WLAN stands for wireless. This is a type of network where the data is not transmitted via cables but over the air through the use of wireless transmitters and receivers.

WLANs are deployed in areas where a wide number of computers may connect to the network but not at the same time. Places like coffee shops often add WLAN to their shops to entice more customers who do not stay for extended periods. Even at home where you have a somewhat fixed number of computers that connect to the network, WLAN is also preferred as it gives users the freedom to move around the house and carry their laptops with them without needing to fuss with cables. For areas where the computers are pretty much fixed, a wired LAN is very desirable due to the advantages that it offers.

First off, a wired LAN is much faster compared to a WLAN. Most wireless routers nowadays are limited to a theoretical maximum speed of 54mbps while a contemporary wired LAN has a bandwidth of 100mbps. Gigabit network equipment can even ramp this up to 1000mbps or 1Gbps. This might not be such a big issue for browsing the internet or sending email but when you are copying large files, it can take a while with a WLAN.

Advantages & disadvantages of wireless LAN

Advantages of WLAN:

- User mobility
- Voice and data services
- Scalable architecture
- Availability of all HiPath VoIP network services
- Access to central applications
- Handover between access points
- Robust model for industry
- Economical access points
- Plug-and-Play architecture

- Robust controller
- Security on the level of fixed networks
- “Small Enterprise” option with own controller
- “Branch Office” option for small branches where remote controller is used

Disadvantages of WLAN:

- As the number of computers using the network increases, the data transfer rate to each computer will decrease accordingly.
- As standards change, it may be necessary to replace wireless cards and/or access points.
- Lower wireless bandwidth means some applications such as video streaming will be more effective on a wired LAN.
- Security is more difficult to guarantee and requires configuration.
- Devices will only operate at a limited distance from an access point, with the distance determined by the standard used and buildings and other obstacles between the access point and the user.
- A wired LAN is most likely to be required to provide a backbone to the WLAN; a WLAN should be a supplement to a wired LAN and not a complete solution.
- Long-term cost benefits are harder to achieve in static environments that require few moves and changes.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain with diagram the architecture of wireless LAN	Jun 2011	7
Q.2	Compare wired & wireless LAN	Jun 2010	7
Q.3	Write comparison between wired LAN, wireless LAN and WIMAX?	Dec 2013	7
Q.4	Test and explain requirements of wireless LAN in detail.	Dec 2012	7
Q.5	Explain wireless LANs and their working	Jun 2014	3.5

UNIT 03/LECTURE 11

WIMAX

Introduction [RGPV/Jun 2011, Dec 2013, Jun 2014]

Worldwide Interoperability for Microwave Access (WiMAX) is currently one of the best technologies in wireless. The Institute of Electrical and Electronics Engineers (IEEE) 802 committee, which sets networking standards such as Ethernet (802.3) and WiFi (802.11), has published a set of standards that define WiMAX. IEEE 802.16-2004 (also known as Revision D) was published in 2004 for fixed applications; 802.16 Revision E (which adds mobility) is publicated in July 2005. The WiMAX Forum is an industry body formed to promote the IEEE 802.16 standard and perform interoperability testing. The WiMAX Forum has adopted certain profiles based on the 802.16 standards for interoperability testing and "WiMAX certification". These operate in the 2.5GHz, 3.5GHz and 5.8GHz frequency bands, whic typically are licensed by various government authorities. WiMAX, is based on an RF technology called Orthogonal Frequency Division Multiplexing (OFDM), which is a very effective means of transferring data when carriers of width of 5MHz or greater can be used. Below 5MHz carrier width, current CDMA based 3G systems are comparable to OFDM in terms of performance. WiMAX is a standard-based wireless technology that provides high throughput broadband connections over long distance. WiMAX can be used for a number of applications, including "last mile" broadband connections, hotspots and high-speed connectivity for business customers. It provides wireless metropolitan area network (MAN) connectivity at speeds up to 70 Mbps and the WiMAX base station on the average can cover between 5 to 10 km.

Typically, a WiMAX system consists of two parts:

- **A WiMAX Base Station** Base station consists of indoor electronics and a WiMAX tower. Typically, a base station can cover up to 10 km radius (Theoretically, a base station can cover up to 50 kilo meter radius or 30 miles, however practical considerations limit it to about 10 km or 6 miles). Any wireless node within the coverage area would be able to access the Internet.
- **A WiMAX receiver** The receiver and antenna could be a stand-alone box or a PC card that sits in your laptop or computer. Access to WiMAX base station is similar to accessing a Wireless Access Point in a WiFi network, but the coverage is more.

Several base stations can be connected with one another by use of high-speed backhaul microwave links. This would allow for roaming by a WiMAX subscriber from one base station to another base station area, similar to roaming enabled by Cellular phone companies.

Several topology and backhauling options are to be supported on the WiMAX base stations: wireline backhauling (typically over Ethernet), microwave Point-to-Point connection, as well as WiMAX backhaul. With the latter option, the base station has the capability to backhaul itself. This can be achieved by reserving part of the bandwidth normally used for the end-user traffic and using it for backhauling purposes.

Advantages over WIFI

WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today.s cell phones. We can compare it with Wi-Fi based on the following factors.

IEEE Standards Wi-Fi is based on IEEE 802.11 standard where as WiMAX is based on IEEE 802.16. However, both are IEEE standards.

Range Wi-Fi typically provides local network access for around a few hundred feet with speeds of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with speeds of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service localWi-Fi networks.

Scalability Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel. WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service
Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Whas is WIMAX? Give technical advantages over WIFI.	Jun 2011	7
Q.2	Explain WIMAX characteristics	Jun 2014	3.5

UNIT 03/LECTURE 12

ETHERNET CABLING

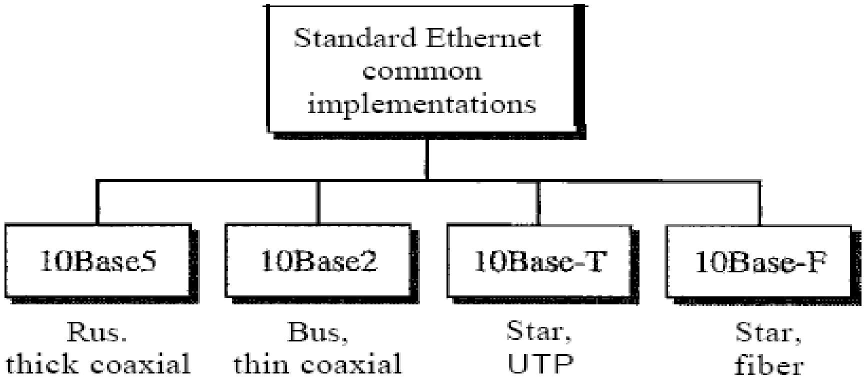


FIGURE 3.23: CATEGORY OF STANDARD ETHERNET

10Base5: Thick Ethernet

The first implementation is called **10BaseS, thick Ethernet, or Thicknet.** The nickname derives from the size of the cable. 10Base5 was the first Ethernet specification to use a bus topology with an external **transceiver** (transmitter/receiver) connected via a tap to a thick coaxial cable.

The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

The maximum length of the coaxial cable must not exceed 500 m; otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

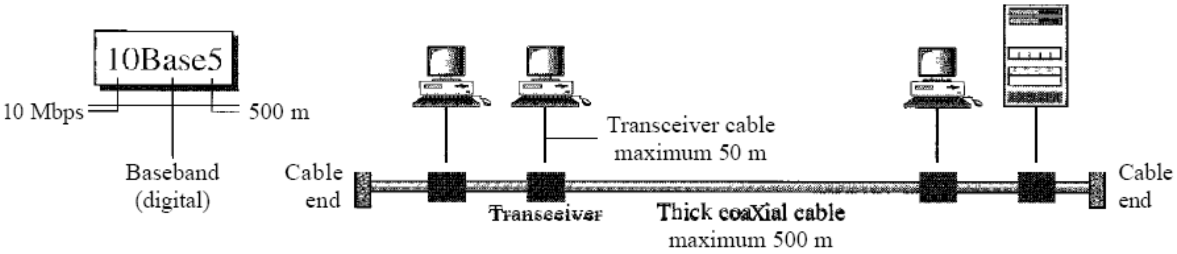


FIGURE 3.24: 10BASE5

10Base2: Thin Ethernet

The second implementation is called 10Base2, **thin** Ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

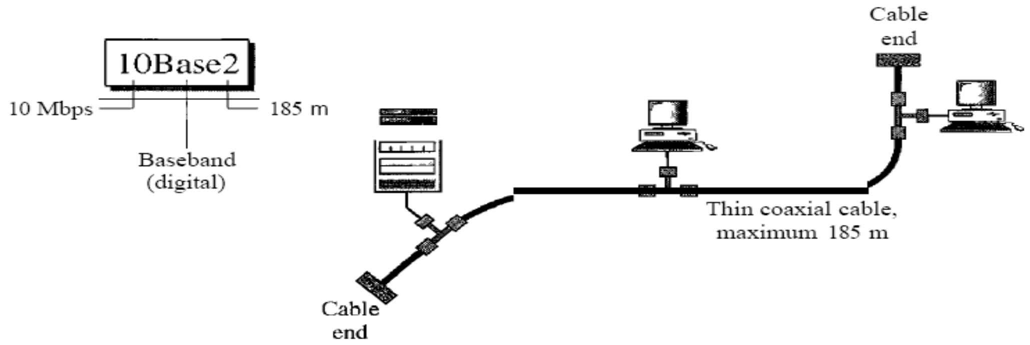


FIGURE3.25 : 10BASE2

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base-T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet. 1OBase-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

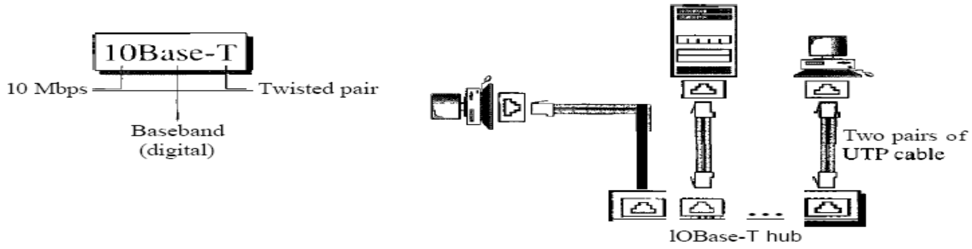


FIGURE 3.26: 10BASET

lOBase-F: Fiber Ethernet

Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.

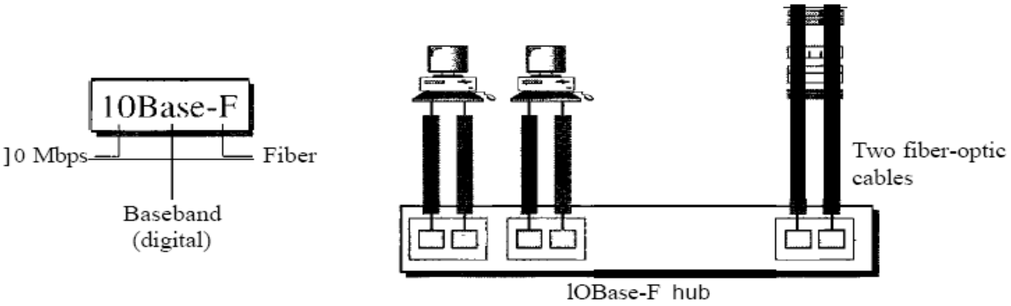
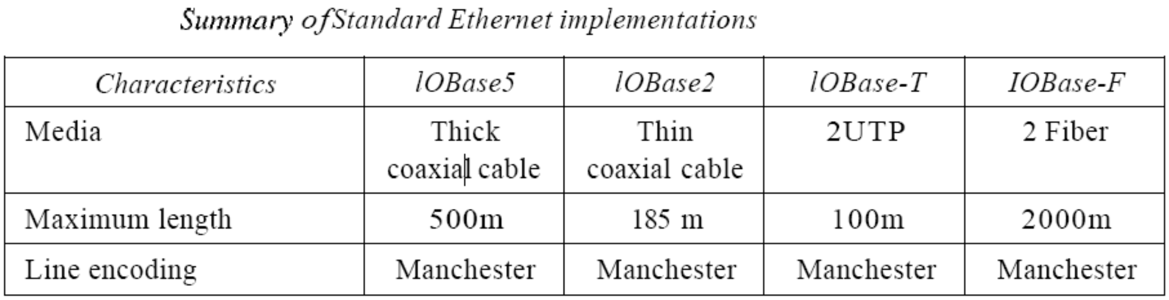


FIGURE 3.27: 10BASEF



Summary ofStandard Ethernet implementations

Characteristics	*lOBase5*	*lOBase2*	*lOBase-T*	*IOBase-F*
Media	Thick coaxial cable	Thin coaxial cable	2UTP	2 Fiber
Maximum length	500m	185 m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester

FIGURE 3.28: SUMMRY OS STANDARD ETHERNET